SCIENTIFIC AMERICAN.COM

September 16, 1996

Subatomic Logic

Researchers nudge closer to the goal of quantum computing

By
Corey S. Powell

The subatomic world, where particles are not solid objects so much as smears of probability, may seem counterintuitive, even illogical. But since the early 1980s, a number of scientists (starting with the late Richard Feynman) have been thinking through schemes to exploit the oddball laws of quantum physics to rational ends; their goal is to create a radically new kind of computer, one far smaller and swifter than any modern silicon device. Though a functional "quantum computer" still lies beyond the grasp of current technology, a succession of theoretical and practical advances suggests some heartening progress toward that goal.

In a quantum computer, information is stored not as a string of ones and zeroes, but as a series of quantum-mechanical states: spin directions of electrons, for instance, or polarization orientations of a photon. In 1985 David Deutsch of the University of Oxford pointed out that quantum physical law allows particles to be in more than one state at a time, making it possible for each particle in a quantum computer to hold more than one bit of information. (In this field, the term "bit" is replaced by "qubit," meaning quantum bit.) A computer containing, say, a hundred particles could execute a computation on 2^{100} numbers at once. The ability to crunch many numbers at the same time--known as massive parallelism--would make quantum computers ideal for some basic computing tasks, such as factoring large numbers. Two years ago, Peter W. Shor of AT&T Bell Labs presented an algorithm showing exactly how a quantum computer would carry out such task.

But there is much more to quantum computers than breaking down large numbers. At last May's ACM Symposium on Theory of Computing, Lov K. Grover, also at Bell Labs, announced a more down-to-earth application: a crafty algorithm that, building on Shor's ideas, would allow a quantum computer to make lightning-fast searches through a database. In this scheme, each item in the database would be represented by a quantum state of a particle in the computer. Relying on the inherently fuzzy laws governing those particles, Grover's algorithm would enhance the state in the system corresponding to the

desired item and suppress the others. Rather than slogging dumbly through a list, the algorithm operates on all of the particles at once, so it could far exceed the speed and efficiency of a classical computer.

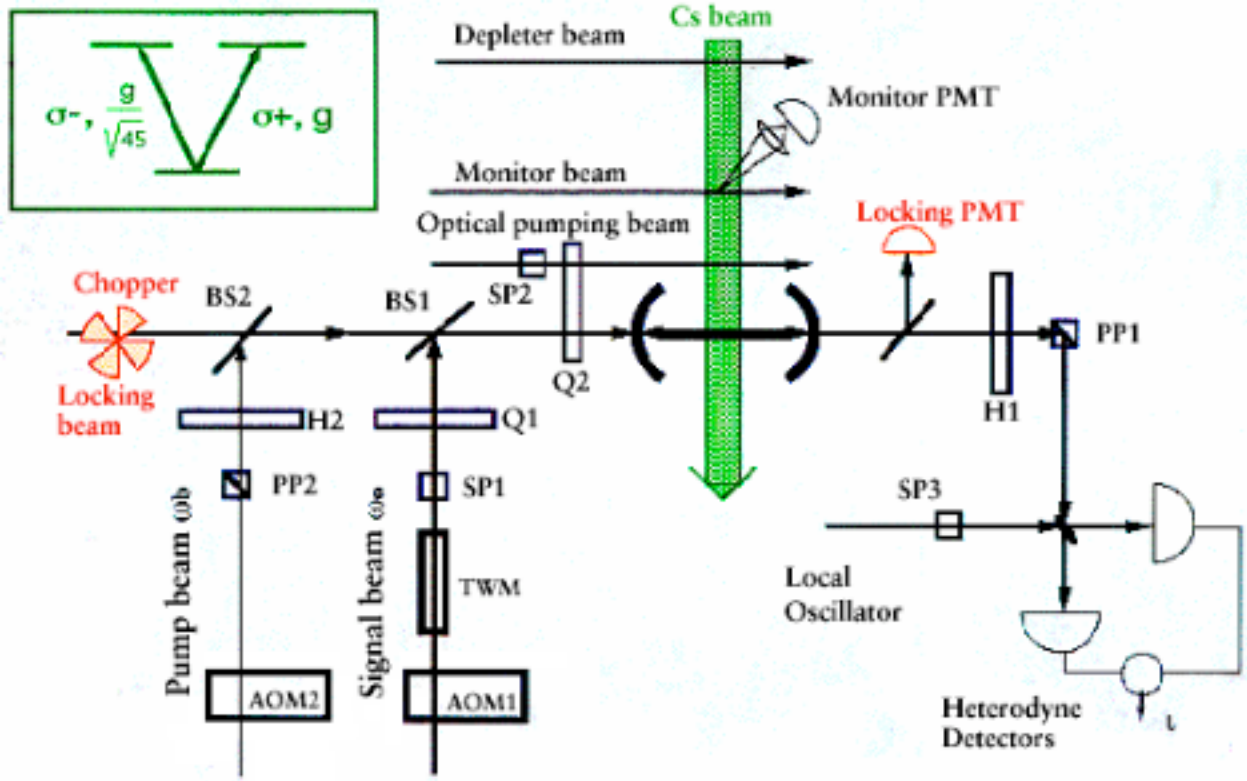
Such list-searching ability could have applications in many other tasks that require finding the optimal member of a set. And a combined talent for factoring and searching may make quantum computers ideal tools for cracking codes (including the Data Encryption Standard, the official U.S. government cryptographic standard).

Another exciting role for quantum computers involves turning them back on their own world and using them to simulate other quantum-mechanical systems--the behavior of quarks in an atomic nucleus, for instance, or electrons in a superconductor. Seth Lloyd of the Massachusetts Institute of Technology is one of the leading researchers working on concrete ways to realize this exotic idea. In essence, the quantum behavior of one set of particles would act as a proxy for that of a different system, bypassing the extraordinarily complex rules of simulation that normally would need to be programmed into a computer.

While nobody is denying the vast potential of quantum computers, even the most ardent enthusiasts are sobered by the obstacles that must be overcome before usable devices can be built. The greatest of these is that the slightest outside disruption--heat or light, for instance--can destroy the balance of quantum states that stores information and makes the computing possible. In technical terms, the system loses its quantum coherence. The very process of reading the state of a qubit can upset the coherence, so retrieving the result of a calculation poses a tough challenge. Even if the system does not fall apart, quantum computers will naturally tend to accumulate errors; the kinds of error-correction schemes developed for classical computers do not translate to the subatomic realm.

Here too, however, there has been substantial recent progress. Shor is working on a method whereby each piece of information is spread, or entangled, over several qubits. In this way, the erroneous decay of one of the quantum states will not lose the information. Of course, using additional qubits trades off some efficiency. Shor's original scheme involved using nine qubits. More recently, Raymond Laflamme and his colleagues at Los Alamos National Laboratory have derived an error-correction technique that requires only five qubits. Shor is also studying how much error is allowable before it taints the results from quantum computers; in essence, proponents of quantum computing are trying to reinvent from the ground up all of the basic logic problems that other computer scientists have developed since the days of ENIAC, the ancestor of the modern electronic computer.

And the programmers working on ENIAC had a significant advantage over Shor and his ilk: they at least had a physical device to work with. Researchers at the National Institute of Standards and Technology, led by David J. Wineland, and a team headed by H. Jeff Kimble at the California Institute of Technology have made some headway in constructing real quantum systems that function as crude logic gates--sort of nano-transistors. These are only the first baby steps toward a full, workable quantum computer.



Source: CALIFORNIA INSTITUTE OF TECHNOLOGY.

Research on computing at the atomic level still involves room-size apparatus. This schematic diagram illustrates an experimental setup.

Nevertheless, many people are betting the technical hurdles are manageable. Researchers at M.I.T., Caltech and the University of Southern California have banded together to form the Quantum Information and Computing institute. The Defense Department's Advanced Research Projects Agency (ARPA) is providing a five-year, $5-million grant--a skinny slice of the total defense R&D pie, but a sign of faith that quantum computing will eventually find a place in our macroscopic lives.